UNITED STATES DISTRICT COURT

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA,)
) Case No: 1:08mj 599
v.)
) **UNDER SEAL**
ABEL NNABUE,)

Affidavit in Support of a Criminal Complaint

I, Hadley Etienne, being duly sworn depose, say, and provide the following information:

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") assigned to the Criminal Computer Intrusion Squad of the Washington Field Office. I have been employed by the FBI for approximately three years. I have over twelve years of experience working with computers, to include five years as a computer programmer, and over seven years as a system/network engineer. As a Special Agent of the FBI, I am authorized to investigate crimes involving computer intrusions, Internet fraud and identity theft.

2. I make this affidavit in support of a criminal complaint charging that TOBECHI ONWUHARA, ABEL NNABUE, PAULA GIPSON, PRECIOUS MATTHEWS, BEN KALU, OBINNA NNEJI, EZENWA ONYEDEBELU, and DONALD OKORO (collectively the Target Subjects) did, in the Eastern District of Virginia, commit offenses against the United States in violation of Title 18, United States Code, Section 1349 (Conspiracy to Commit Bank Fraud).

3. The information in this affidavit is based on (1) my personal knowledge and observations during the course of this investigation; (2) information conveyed to me by other law enforcement officials; (3) review of the evidence obtained from search warrants, pen registers and trap and trace devices, and subpoenas; (4) my review of call recordings; and (5) interviews with the

Target Subjects. Since this affidavit is submitted for the limited purpose of establishing probable cause, I have not set forth each and every fact known regarding this investigation.

DEFINITIONS OF COMPUTER-RELATED TERMS

4. The "Internet" is a collection of computers that are connected to one another via high-speed data links and telephone lines for the purpose of sharing information and services. Connections between Internet computers may exist across state and international borders, even if those computers are in the same state.

5. Electronic mail (email) is a popular form of transmitting messages and/or files in an electronic environment between computer users. An Internet Protocol Address ("IP address") is a unique numeric address used to identify computers on the Internet. An IP address is comprised of a series of four numbers, each in the range of 0-255, separated by periods (e.g., 10.212.8.177). Every computer connection to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer is directed properly from its source to its destination. An IP address acts much like a home or business street address - it enables Internet sites to properly route traffic to each other.

6. An Internet Protocol Address ("IP address") is a unique numeric address used to identify computers on the Internet. An IP address is comprised of a series of four numbers, each in the range of 0-255, separated by periods (e.g., 10.212.8.177). Every computer connection to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer is directed properly from its source to its destination. An IP address acts much like a home or business street address - it enables Internet sites to properly route traffic to each other.

7. Broadband Internet access refers to relatively high-speed connections allowing access to other computers on the Internet. Normally, the standard is a dial-up connection, while significantly faster connections are considered "broadband."

8. Wireless Internet access is accomplished without a physical cable attaching the computer to a network, e.g. the Internet, an Internet Service Provider, or a local network of some kind. Wireless cards allow a computer to connect to a local wireless hub in a home or business, or to a Wireless Cellphone Provider's network using cell towers. The wireless card and wireless receiver communicate by transmitting radio signals.

9. Caller-ID is a service provided by phone companies that displays the phone number of the caller on the receiver's phone or a special Caller-ID box. The display normally includes the caller's number and, if available, the directory listing for the caller, e.g. caller's name or business name.

THE SUBJECTS

10. TOBECHI ONWUHARA (ONWUHARA) is primarily responsible for calling financial institutions and convincing them to wire transfer money out of victims' accounts. ONWUHARA also organizes others who make such calls. ONWUHARA splits his time between Miami, Florida and Dallas, Texas. ONWUHARA is also known as Tobe or T.

11. ABEL NNABUE (NNABUE) is primarily responsible for identifying potential victims and coordinating the gathering of information on victims. NNABUE resides in Dallas, Texas. NNABUE is also known as Que or Q.

12. PAULA GIPSON (GIPSON) is primarily responsible for calling financial institutions and convincing them to wire transfer money out of victims' accounts and obtaining information on victims. GIPSON resides in Dallas, Texas.

13. PRECIOUS MATTHEWS (MATTHEWS) is primarily responsible for calling financial institutions and convincing them to wire transfer money out of victims' accounts and laundering the proceeds of the scheme. MATTHEWS is ONWUHARA's fiancée and lives in Miami, Florida.

14. BEN KALU (KALU) is primarily responsible for providing information on victims. KALU lives in Baltimore, Maryland.

15. OBINNA NNEJI (NNEJI) is primarily responsible for laundering money. NNEJI resides in Houston, Texas.

16. EZENWA ONYEDEBELU (ONYEDEBELU) is primarily responsible for laundering money. ONYEDEBELU resides in Dallas, Texas.

17. DONALD OKORO (OKORO) is primarily responsible for laundering money. OKORO resides in Dallas, Texas.

18. MIKE WALTER (WALTER) is primarily responsible for organizing money mules in Asia and transferring the money back to the Target Subjects. WALTER resides in Jakarta, Indonesia and was arrested in Singapore as a result of this scheme in or about July 15, 2008.

THE SCHEME

19. The Target Subjects are engaged in a scheme designed to defraud financial institutions. The Target Subjects normally target victims who have a large balance in a Home Equity Line of

Credit (HELOC). The Target Subjects use the fraudulently-obtained personal information of the victims to initiate wire-transfers to over-seas bank accounts without the knowledge or authorization of the victims. Although each case is a little different, the following are the primary steps in the scheme.

20. The Target Subjects obtained pre-paid cell phones, Yahoo! email accounts, pre-paid wireless broadband PC cards, accounts with J2 Global Communications (J2), a fax-to-email service, accounts with E&M Enterprises (d/b/a/ Spoofcard.com) (Spoofcard), a Caller-ID spoofing service, and accounts with Listsource, a company that provides mortgage and real estate information.

21. NNABUE and others used Listsource to gather mortgage and real estate information, including information on potential victims who had large HELOC accounts. They would then make a copy of the victim's signature from the lease or loan documents. GIPSON, KALU, and others would then run credit reports on the victims. The credit reports would show available balances on the HELOC accounts, as well as other personal information.

22. The Target Subjects would then use a pre-paid cell phone to call the victim's phone company and forward the victim's phone number to the pre-paid cell phone. The Target Subjects would use Spoofcard to make it appear that the call originated from the victim's phone.

23. ONWUHARA, GIPSON, MATTHEWS, and others would call the victim's financial institution, normally a credit union, and use social engineering to obtain account information, including account numbers, balances, passwords, security questions, and the like. In some cases, the Target Subjects would use a laptop computer hooked up to a pre-paid wireless broadband

card to access the victim's account over the Internet, using information obtained through the calls to the financial institution.

24. ONWUHARA, GIPSON, MATTHEWS, and others would then request a wire transfer from the victim's account to a bank account in Asia. As part of the financial institution's normal procedure, they would either fax or email an authorization form to the subjects. The Target Subjects would either have the form faxed to a number at J2 that would in turn email the form to the subjects, or they would have the bank email it to one of their Yahoo! accounts. The Target Subjects would fill out the form and cut and paste the electronic version of the victim's signature that they had previously acquired from Listsource. The Target Subjects would then fax the form back to the bank, normally through J2, sometimes including a header at the top that made it appear that the fax came from the victim's phone.

25. Money transferred to banks in Asia was collected by money mules who got a cut of the incoming funds in return for opening business accounts, receiving money via wire transfers into those accounts, and then withdrawing the money and turning it over to couriers. The couriers bundled the money into containers and shipped the money to WALTER. WALTER would then send money transfers, normally via Western Union, to the Target Subjects, in amounts ranging from a thousand dollars up to tens of thousands of dollars. In addition, WALTER would send large transfers to ONWUHARA, including a transfer of €40,000,000.

26. MATTHEWS would transfer some of the money received to others, including ONYEDEBELU, NNEJI, GIPSON, NNABUE, and OKORO. In addition, ONWUHARA would go to casinos and deposit large sums of money, often in the hundreds of thousands of dollars.

Days later, ONWUHARA would cash out approximately the same amount of money in the form of checks.

PROBABLE CAUSE

27. At 12:24 pm on December 7, 2007, an unidentified individual, impersonating Robert Short, called USSFCU, provided the correct personal information of Mr. Short and requested to make a wire transfer in the amount of $280,000 dollars from Mr. Short's savings account to a Woori Bank of Korea account, ending in #1001, through the Wachovia Bank of New York.

28. As part of their normal business practice, USSFCU sent a wire transfer form to the caller. The caller asked that the form be sent to allstateassociates@yahoo.com. Upon receipt of the completed form, USSFCU sent the wire transfer to the Wachovia Bank of New York, and the Wachovia Bank in turn wired the fund to the Woori Bank of Korea. The call was recorded as the regular business practice of the USSFCU, and was provided to the USSS and the FBI. Both Mr. Short and USSFCU are located in Alexandria, within the Eastern District of Virginia.

29. On December 9, 2007, the true Robert Short attempted to log onto the USSFCU Internet online banking but was not able to gain access due to a problem with the password. On December 10, 2007, Mr. Short contacted the USSFCU and was provided with a new password. Upon logging onto the Internet online banking, Mr. Short noticed that a total of $280,000 dollars was missing and that several unauthorized Internet online transactions had been conducted in the checking account, the savings account and the Home Equity Line of Credit ("HELOC") account. Mr. Short notified the USSFCU of the discovery.

30. Pursuant to a subpoena, USSFCU provided the IP address that connected to Short's online account. The IP address came back to a pre-paid Verizon Wireless Broadband card with mobile telephone number (MTN) (954) 892-7434. In addition, Yahoo! Inc. ("Yahoo!"), in response to a subpoena, provided the same IP address as having accessed the email account: allstateassociates@yahoo.com.

31. Pursuant to a subpoena, Verizon provided video footage showing three men depositing $200 in cash at a Verizon store in Plano, Texas for the Verizon broadband account with MTN (954) 892-7434. A cooperating witness, who was a former associate with ONWUHARA and NNABUE, identified ONWUHARA and NNABUE as two of the three individuals in the video footage from Verizon.

32. Further investigation revealed that the Target Subjects were using the services of Spoofcard, a company that provides Caller-ID spoofing, call recording, and voice masking services. The Target Subjects would call Spoofcard's toll-free number and enter a PIN. They would then specify the recipient's phone number and the number they wished to display on the recipient's Caller-ID box.

33. The investigation has also uncovered additional victim banks and credit unions in which the same methods, Spoofcard PINs, e-mail addresses, and pre-paid cell phones have been used to conduct the fraud. Pursuant to a search warrant issued by this Court, the FBI and USSS have obtained and listened to recordings of calls made by the Target Subjects. The agents were able to differentiate the voices of several men and two women.

34. A review of telephone recordings provided by Spoofcard identified a call placed on November 10, 2007 at approximately 17:49 EST, from the same individual who called USSFCU on December 7, 2007. The caller used the Spoofcard service to disguise his telephone number,

214-240-9841, as that of a local physician. The subject contacted CVS Pharmacy, 3900 Forest Lane, Dallas, Texas, impersonated Dr. Mc Elya, and made a request for a prescription of Valtrex (500mg) for TOBE ONWUHARA.

35. On November 17, 2007 at approximately 18:50:40 EST, the same individual again used the Spoofcard service to disguise telephone number 214-240-9841. This time the subject contacted CVS Pharmacy, 4610 Frankfort Road Dallas, Texas and impersonated Dr. McElya to request a prescription of Valtrex (500 mg). The prescription was to be picked up by TOBE ONWUHARA, using ONWUHARA's birth date.

36. Another recording was of ONWUHARA placing a call from his cell phone, 214-240-9841, to GIPSON at 214-663-1509 on November 26, 2007. GIPSON stated that "she had two that were open" (bank accounts). During the call ONWUHARA asked GIPSON if she had completed transactions that they previously discussed. ONWUHARA and GIPSON discussed a scheme where they would need to physically go inside of Wachovia Banks and open a business account. ONWUHARA stated that he knew someone that worked for Chicago Department of Motor Vehicles (CDMV) who could provide valid Chicago driver license bearing any name or address provided. ONWUHARA also stated that the individual provides the driver's license to help people who may not have "papers." ONWUHARA told GIPSON that she would need to be in the CDMV between 12:30 pm and 4:00 p.m.

37. Pursuant to a subpoena, Cingular Wireless provided registration information showing that the wireless phone number 214-663-1509 was registered to PAULA GIPSON.

38. During the review of the Spoofcard recordings, it was revealed that on September 7, 2007, GIPSON placed a telephone call to a victim financial institution. After providing the security verification information, GIPSON obtained the victim's account balance. GIPSON also verified

to see if a wire transfer had been taken out of the account.

39. Pursuant to a search warrant issued from the Eastern District of Virginia, Yahoo provided copies of messages sent and received from allstateassociates@yahoo.com. The messages included messages to and from p08g75@yahoo.com. Pursuant to a grand jury subpoena, Yahoo provided the account profile for the p08g75@yahoo.com email account, showing that it is was registered to Paula R. Gipson of Dallas, Texas. Yahoo also provided the IP address used to access the account. The IP address that accessed the account was used by Paula Gipson and a company she runs, Extra Mile Enterprise.

40. In another email to Q at the allstateassociate@yahoo.com email address, GIPSON stated that she had an address that Q could use to receive mail. GIPSON provided the address: 911 Edgedale, Dallas, Texas 75232, and added that no one lived there, but it was setup to look like someone lived at the address. GIPSON stated that she checks the mail on occasions, but if Q sent mail to the address, he should let her know.

41. On April 10, 2008, pursuant to a sneak-and-peek search warrant issued by United States Magistrate Judge Joan M. Azrack, Eastern District of New York, ONWUHARA, NNABUE, MATTHEWS, and a traveling companion were stopped together and interviewed at JFK International Airport on their return to the United States from Nigeria. During a conversation with ONWUHARA, your affiant recognized ONWUHARA's voice as the same voice on calls to USSFCU on December 7, 2007 that resulted in the fraudulent and unauthorized transfer of $280,000 from the account of Robert Short. ONWUHARA was in possession of the cellular telephone with phone number 214-240-9841 at the time of the interview.

42. On the same date, during a conversation with MATTHEWS, MATTHEWS confirmed that ONWUHARA went by the nickname T or Tobe, and that NNABUE went by the nickname

Q or Que. Your affiant recognized MATTHEWS's voice as one of the female callers on calls to financial institutions requesting wire transfers.

43. Pursuant to a search warrant, Yahoo! provided the contents of the mailbox allstateassociates@yahoo.com. Among other messages, the mailbox contained the following:

a. On December 18, 2007, the allstateassociates@yahoo.com account received an order confirmation email from ListSource.com. ListSource is one of the nation's largest sources for property and mortgage data. The data provided by ListSource comes from county assessment files, updated with recorded deed transactions and mortgages. It is believed that ListSource.com data is being used to identify potential victims. The evidence suggests that once the victim is identified and targeted, the signatures from the deed documents are copied onto the signature portion of the wire transfer authorization forms.

b. On July 29, 2006, an email containing victim account information was sent to a co-conspirator. The co-conspirator was asked to "take care of this one" and NNABUE explained that the funds could be shared. The email was signed "QUE."

c. On September 7, 2006, KALU sent a victim's personal data from his email account benkalu2000@yahoo.com. The reply email in reference to the personal data stated that the social security number and birthday would need to be provided before they could proceed. The email was signed "QUE."

d. On September 14, 2007, QUE emailed a copy of a victim's Equifax credit file to a co-conspirator.

e. On November 28, 2006, a co-conspirator sent an email stating that he knew someone that could provide HELOC accounts, but required a 50-50 sharing pattern. On

December 6, 2006, a reply to the email stated: "hello there, this is QUE i have not heard from u since our last conversation about the percentage. Lets try to work on something as soon as we can."

44.

45. Pursuant to a search warrant issued by this Court Yahoo! provided the contents of the email account benkalu2000@yahoo.com. The contents included a message from KALU's wife requesting that divorce papers be sent to a specified address. The message included a copy of some of KALU's financial documents.

46. Pursuant to a search warrant, Yahoo! provided the contents of email account tobeohara@yahoo.com, which had received email from allstateassociates@yahoo.com in reference to the current scheme. The contents of the account included messages to an individual in Indonesia named "Mike." The individual in Indonesia stated that he could get access to accounts in Korea, China, Hong Kong, Singapore, and Indonesia and would split the proceeds 40% / 60%

47. Suspicious Activity Reports (SARS) show money being sent via wire transfer from Indonesia to MATTHEWS, NNEJI, OKORO, GIPSON, NNABUE, ONYEDEBELU, OKORO, and ONWUHARA. The phone number in Indonesia for all of these transactions was the same (6285697050066). On or about July 15, 2008, police in Singapore arrested six individuals in reference to a lead sent as a result of this investigation. Four of the individuals were identified as money mules, one was identified as MIKE WALTER. WALTER had a cell phone with the same phone number as used in the money transfers to the Target Subjects.

48. Pursuant to a combination search warrant and pen register/trap and trace device, AT&T Wireless provided toll records and location information for the personal cell phones of ONWUHARA, NNABUE, GIPSON, and MATTHEWS for approximately the last month.

49. On July 30, 2008, Cingular/AT&T accidentally provided the name and number of the FBI technician tracking ONWUHARA's phone to ONWUHARA. ONWUHARA called the technician and was told that he had reached the FBI. ONWUHARA stopped taking or receiving calls on his cell phone and began using MATTHEWS's cell phone. ONWUHARA called NNEJI multiple times and NNEJI wire transferred $39,000 to MATTHEWS's bank account, from NNEJI's wife's account. MATTHEWS immediately withdrew $6000 of those funds.

CONCLUSION

50. Based upon the forgoing, I have probable cause to believe from in or about September 2007, and continuing through in or about July 2008, in the Eastern District of Virginia and elsewhere, ABEL NNABUE did knowingly conspire to execute a scheme or artifice to defraud a financial institution and to obtain any of the moneys funds, credits, assets, securities, and other property owned by, and under the control and custody of, a financial institution, by means of false and fraudulent pretenses, representations, and promises, in violation of Title 18, United States Code, Section 1349.

I therefore request a warrant be issued to any duly authorized Officer of the United States to arrest ABEL NNABUE.

Hadley Etienne
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me this 1st day of August, 2008 at Alexandria, VA.

/s/
Barry R. Poretz
United States Magistrate Judge